Guide du routard numérique : Épisode 1

J. Schaeffer [schaeffer@univ-brest.fr]

IUEM

October 5, 2010





Feiri



Sommaire





Définition

Definition

Un mot de passe est un moyen d'authentification pour utiliser une ressource ou un service dont l'accès est limité et/ou protégé.





Définition

Definition

Un mot de passe est un moyen d'authentification pour utiliser une ressource ou un service dont l'accès est limité et/ou protégé. C'est une série de caractères (lettres, chiffres ou caractères spéciaux) tenus secret et connu de l'utilisateur seul.





Robustesse d'un mot de passe

Elle se mesure sur trois critères





Robustesse d'un mot de passe

Elle se mesure sur trois critères

- la taille (en nombre de caractères)





Robustesse d'un mot de passe

Elle se mesure sur trois critères

- la taille (en nombre de caractères)
- la diversité des caractères utilisés




Robustesse d'un mot de passe

Elle se mesure sur trois critères

- la taille (en nombre de caractères)
- la diversité des caractères utilisés
- la durée de vie





Les mauvais mots de passe

Exemple de mauvais mots de passe

- moins de 8 caractères





Les mauvais mots de passe

Exemple de mauvais mots de passe

- moins de 8 caractères
- trop de caractères identiques





Les mauvais mots de passe

Exemple de mauvais mots de passe

- moins de 8 caractères
- trop de caractères identiques
- termine par deux chiffres





Les mauvais mots de passe

Exemple de mauvais mots de passe

- moins de 8 caractères
- trop de caractères identiques
- termine par deux chiffres

Example

toto, toto65, js090980, tursiop, AZERTY123 ...





Les bons mots de passe

Caractéristiques d'un bon mot de passe





Les bons mots de passe

Caractéristiques d'un bon mot de passe

- Au moins 8 caractères chiffres et lettres





Les bons mots de passe

Caractéristiques d'un bon mot de passe

- Au moins 8 caractères chiffres et lettres
- Au moins 2 caractères spéciaux (ponctuations, caractères nationaux ...)




Les bons mots de passe

Caractéristiques d'un bon mot de passe

- Au moins 8 caractères chiffres et lettres
- Au moins 2 caractères spéciaux (ponctuations, caractères nationaux ...)
- Pas un mot du dictionnaire





Les bons mots de passe

Caractéristiques d'un bon mot de passe

- Au moins 8 caractères chiffres et lettres
- Au moins 2 caractères spéciaux (ponctuations, caractères nationaux ...)
- Pas un mot du dictionnaire

Ajouter une lettre majuscule et un astérisque à un mot de passe de 8 caractères augmente le temps de calcul de 2 jours à 2 siècles.





Sommaire





Le drame du vol des mots de passe

- usurpation d'identité





Le drame du vol des mots de passe

- usurpation d'identité
- vol de numéro de cartes bleues





Le drame du vol des mots de passe

- usurpation d'identité
- vol de numéro de cartes bleues
- source de spam




Le drame du vol des mots de passe

- usurpation d'identité
- vol de numéro de cartes bleues
- source de spam
- vol de clé WiFi





Le drame du vol des mots de passe

- usurpation d'identité
- vol de numéro de cartes bleues
- source de spam
- vol de clé WiFi
- dégâts dépassant l'individu





Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.





Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.




Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.
Les mots de passes les plus vulnérables sont :

- les mots du dictionnaire





Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.
Les mots de passes les plus vulnérables sont :

- les mots du dictionnaire
- deux mots du dictionnaire concaténés





Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.
Les mots de passes les plus vulnérables sont :

- les mots du dictionnaire
- deux mots du dictionnaire concaténés
- les mots du dictionnaire avec la règle de remplacement des caractères (i devient !; o devient 0 ; etc.)





Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.
Les mots de passes les plus vulnérables sont :

- les mots du dictionnaire
- deux mots du dictionnaire concaténés
- les mots du dictionnaire avec la règle de remplacement des caractères (i devient !; o devient 0 ; etc.)
- les mots du dictionnaires suivis de deux chiffres




Force Brute

Les attaques les plus courantes sont dites de "force brute" et consistent à essayer toutes les combinaisons possibles.
Ces attaques semblent naïves mais elles sont TRÈS efficaces.
Les mots de passes les plus vulnérables sont :

- les mots du dictionnaire
- deux mots du dictionnaire concaténés
- les mots du dictionnaire avec la règle de remplacement des caractères (i devient !; o devient 0 ; etc.)
- les mots du dictionnaires suivis de deux chiffres
- le nom (ou initiales) suivis de 4 ou 6 chiffres





Quelques chiffres

À partir d'un PC standard moderne, on calcule environ 10^7 mots de passe par secondes.

- Sur un alphabet de 26 caractères, un mot de passe longueur 6 (300 millions de combinaisons possibles) tient au maximum ...





Quelques chiffres

À partir d'un PC standard moderne, on calcule environ 10^7 mots de passe par secondes.

- Sur un alphabet de 26 caractères, un mot de passe longueur 6 (300 millions de combinaisons possibles) tient au maximum ...
- 30 secondes





Quelques chiffres

À partir d'un PC standard moderne, on calcule environ 10^7 mots de passe par secondes.

- Sur un alphabet de 26 caractères, un mot de passe longueur 6 (300 millions de combinaisons possibles) tient au maximum ...
- 30 secondes
- Mais pour un mot de longueur 8 (200 milliards de combinaisons possibles), cela devient ...





Quelques chiffres

À partir d'un PC standard moderne, on calcule environ 10^7 mots de passe par secondes.

- Sur un alphabet de 26 caractères, un mot de passe longueur 6 (300 millions de combinaisons possibles) tient au maximum ...
- 30 secondes
- Mais pour un mot de longueur 8 (200 milliards de combinaisons possibles), cela devient ...
- 350 minutes





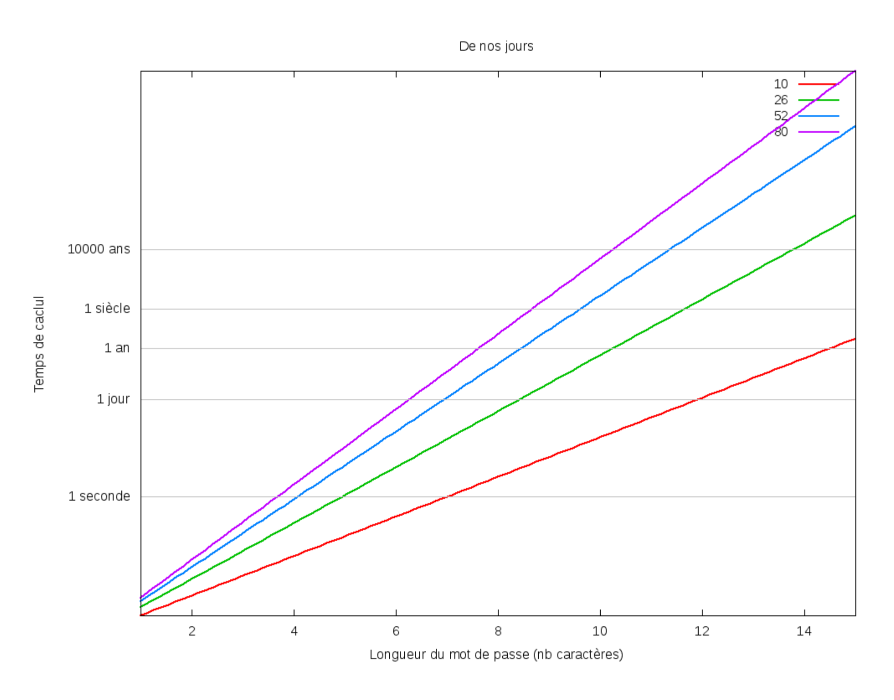
Quelques chiffres

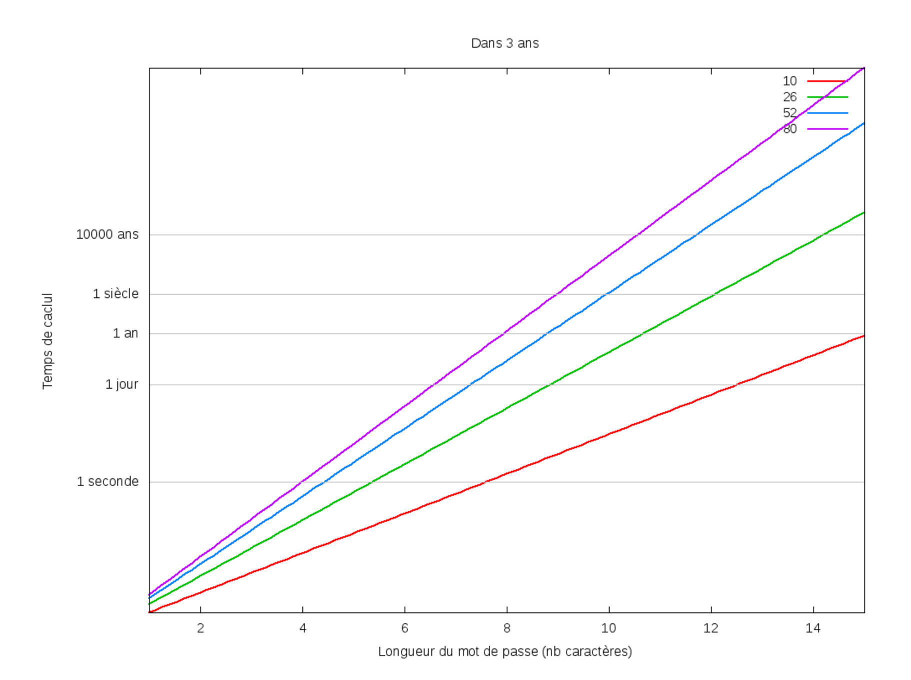
À partir d'un PC standard moderne, on calcule environ 10^7 mots de passe par secondes.

- Sur un alphabet de 26 caractères, un mot de passe longueur 6 (300 millions de combinaisons possibles) tient au maximum ...
- 30 secondes
- Mais pour un mot de longueur 8 (200 milliards de combinaisons possibles), cela devient ...
- 350 minutes
- On teste tous les mots du dictionnaire français (350000 × 2) en moins d'une seconde.

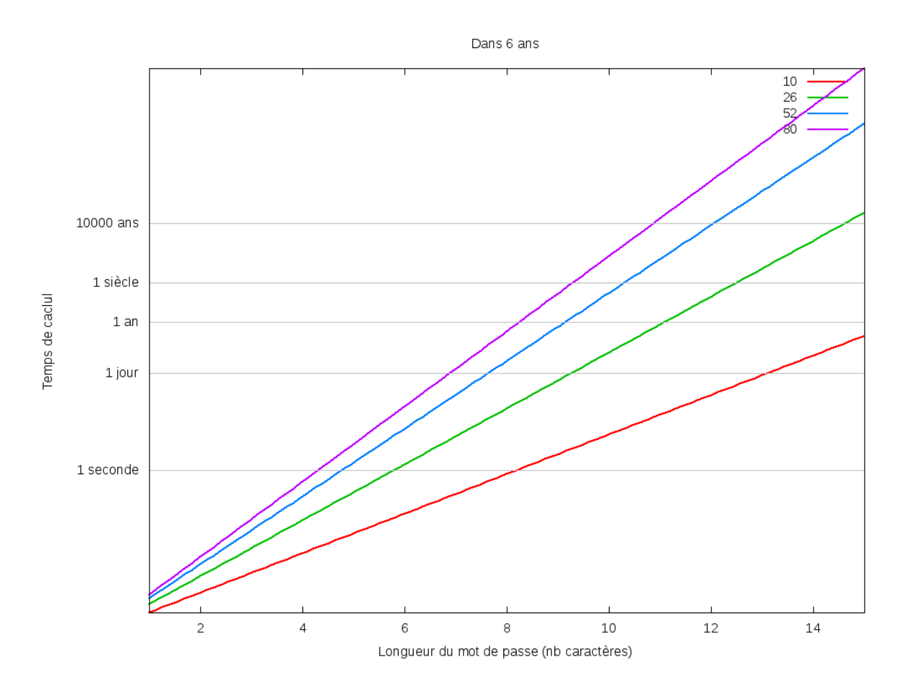





De nos jours
10
26
52
80
10000 ans
1 siècle
1 an
1 jour
1 seconde
Temps de caclul
2
4
6
8
10
12
14
Longueur du mot de passe (nb caractères)



Dans 3 ans
10
26
52
80
10000 ans
1 siècle
1 an
1 jour
1 seconde
Temps de caclul
2
4
6
8
10
12
14
Longueur du mot de passe (nb caractères)


Dans 6 ans
10
26
52
80
10000 ans
1 siècle
1 an
1 jour
1 seconde
Temps de caclul
2
4
6
8
10
12
14
Longueur du mot de passe (nb caractères)

exemple de l'UBO

- On récupère la liste des utilisateurs (trivial, par l'annuaire)





exemple de l'UBO

- On récupère la liste des utilisateurs (trivial, par l'annuaire)
- On fait des hypothèses fortes sur un type de mot de passe (2 lettres minuscules et 4 chiffres)





exemple de l'UBO

- On récupère la liste des utilisateurs (trivial, par l'annuaire)
- On fait des hypothèses fortes sur un type de mot de passe (2 lettres minuscules et 4 chiffres)
- Cela représente $26^2 \times 10^4 = 676.10^6$ possibilités par compte.




exemple de l'UBO

- On récupère la liste des utilisateurs (trivial, par l'annuaire)
- On fait des hypothèses fortes sur un type de mot de passe (2 lettres minuscules et 4 chiffres)
- Cela représente $26^2 \times 10^4 = 676.10^6$ possibilités par compte.
- Pour les 3000 comptes à l'UBO (d'après l'annuaire LDAP), cela donne 2.10^{12} (2000 milliards) essais pour attaquer tous les comptes.




exemple de l'UBO

- On récupère la liste des utilisateurs (trivial, par l'annuaire)
- On fait des hypothèses fortes sur un type de mot de passe (2 lettres minuscules et 4 chiffres)
- Cela représente $26^2 \times 10^4 = 676.10^6$ possibilités par compte.
- Pour les 3000 comptes à l'UBO (d'après l'annuaire LDAP), cela donne 2.10^{12} (2000 milliards) essais pour attaquer tous les comptes.
- $2.10^{12}/10^7 = 2.10^5$ secondes, soit 5 heures de calcul.





Définition

Definition

La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. (Extrait de Wikipedia)




Exemples

De : PayPal Accounts <accounts@newsalert.net>
Objet : **Votre acces de compte est limite**
Date : 26 février 2009 17:07:22 HNE
Répondre à : noreply@newsalert.net



Cher membre de **PayPal®**,

Pendant un criblage récent, nous avons détecté une erreur dans votre information de facturation sur le dossier.

Ouvrez une session svp en votre compte maintenant et évitez les limitations qui pourraient être imposées à votre compte.
Connectez-vous

http://constant2ensurance.grapeape.org/maison.html

Merci de votre attention prompte à cette matière. Comprenez svp que c'est une mesure de sécurité prévue pour aider à protéger vous et votre compte. Nous sommes désolés pour le dérangement.

Cordialement,
PayPal

Exemples


*** PROBABLY SPAM *** Banque Postale: Désactivation de votre carte de crédit. - Courrier entrant -
Fichier Édition Affichage Aller à Messages Outils Aide
Relever
Écrire
Adresses
Étiquette
Rechercher dans to
Courrier entrant - Dossiers locaux
*** PROBABLY SPAM ***...
répondre
de La Banque Postale. <service@PayPal.Fr>
sujet *** PROBABLY SPAM *** Banque Postale: Désactivation de votre carte de crédit.
pour Vous-même
LA BANQUE POSTALE
Relevé de compte de La Banque Postale
Désactivation de votre carte de crédit.
Bonjour,
Nous venons de désactiver votre carte de crédit.
Pour le réactiver, vous devez vous connecter sur le site de La Banque Postale et accéder à votre espace sécurisé de Banque en Ligne via le lien ci-dessous en saisissant vos identifiant et mot de passe ainsi que votre carte de crédit.
https://www.labanquepostale.fr/index/particuliers/banque_en_ligne/identification/reactivation=452266
Ce =message est généré automatiquement, ne répondez pas à l'expéditeur.
Si vous n'êtes pas destinataire(s) de ce message, merci de le détruire.
La Banque Postale, Société Anonyme à Directoire et Conseil de Surveillance, au capital de 2 342 454 090 euros
Siège social : 115, rue de Sèvres - 75275 Paris Cedex 06 - RCS Paris 421 100 645 - Code A.P.E 6419Z.
© La Banque Postale 2010
La Banque Postale :
"Le papier est un bien précieux, ne le gaspillez pas. N'imprimez ce document que si vous en avez vraiment besoin !"
Ce message est confidentiel.
http://christie-stephen.lovingu.hk/banque-postale.fr/

Sommaire




Créez votre mot de passe

Quelques idées :

- les initiales d'une phrase : "Sauvez les Bretons : mangez 5 cochons par jour !" ⇒ "SIB:m5c/j!"




Créez votre mot de passe

Quelques idées :

- les initiales d'une phrase : "Sauvez les Bretons : mangez 5 cochons par jour !" ⇒ "SIB:m5c/j!"
- utilisez systématiquement un générateur de mots de passes




Créez votre mot de passe

Quelques idées :

- les initiales d'une phrase : "Sauvez les Bretons : mangez 5 cochons par jour !" ⇒ "SIB:m5c/j!"
- utilisez systématiquement un générateur de mots de passes
- trouver votre logique propre




Conseils d'utilisation

- Faites confiance à votre mémoire





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier
  - à la première page d'un cahier





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier
  - à la première page d'un cahier
  - dans un fichier de votre ordinateur





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier
  - à la première page d'un cahier
  - dans un fichier de votre ordinateur
- Si vous devez absolument l'écrire, transformez le légèrement et mettez les dans un tiroir fermé à clé





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier
  - à la première page d'un cahier
  - dans un fichier de votre ordinateur
- Si vous devez absolument l'écrire, transformez le légèrement et mettez les dans un tiroir fermé à clé
- Mieux encore, utilisez un logiciel qui génère des mots de passe et les stocke dans un fichier chiffré





Conseils d'utilisation

- Faites confiance à votre mémoire
- Sinon, ne l'écrivez pas
  - sur un papier sur votre bureau ou sous le clavier
  - à la première page d'un cahier
  - dans un fichier de votre ordinateur
- Si vous devez absolument l'écrire, transformez le légèrement et mettez les dans un tiroir fermé à clé
- Mieux encore, utilisez un logiciel qui génère des mots de passe et les stocke dans un fichier chiffré
- Utilisez beaucoup de mots de passe différents




Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)

Avantages





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)

Avantages

- À chaque service son mot de passe, on les retrouve facilement





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)

Avantages

- À chaque service son mot de passe, on les retrouve facilement
- Ils sont en sécurité (faites une copie de ce fichier)





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)

Avantages

- À chaque service son mot de passe, on les retrouve facilement
- Ils sont en sécurité (faites une copie de ce fichier)

Inconvenients





Logiciel de gestion de mots de passe

- Génère des mots de passe aléatoires
- Stocke les mots de passes dans un fichier chiffré
- Un mot de passe maitre pour accéder à votre catalogue de mots de passe (attention à ce qu'il soit fort)

Avantages

- À chaque service son mot de passe, on les retrouve facilement
- Ils sont en sécurité (faites une copie de ce fichier)

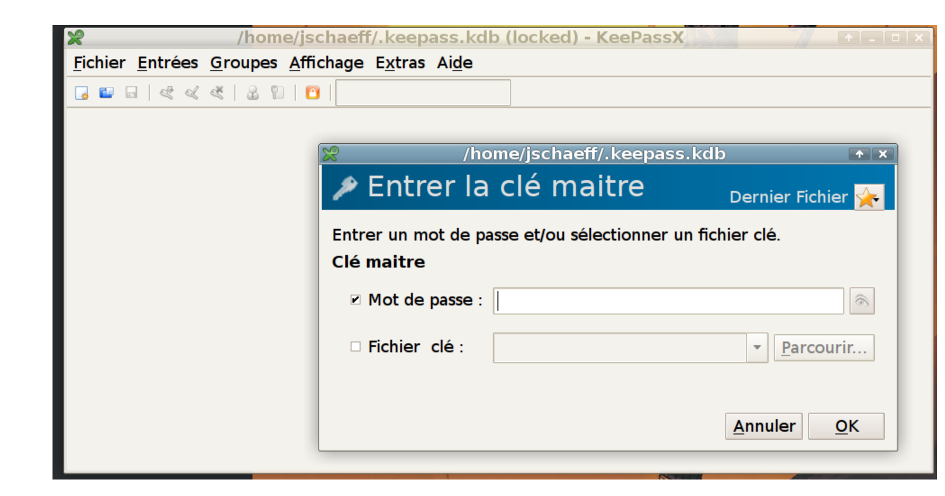
Inconvenients

- Difficile à utiliser sur plusieurs postes (on peut se servir d'une clé USB)

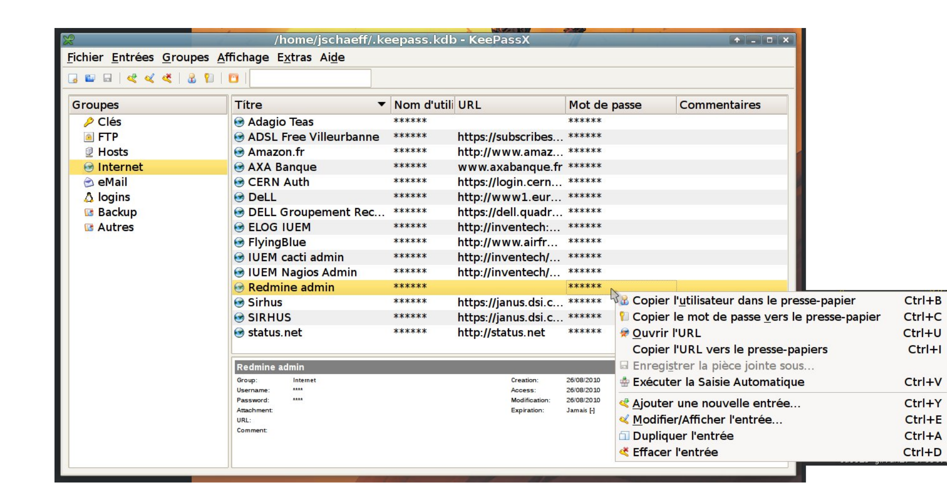




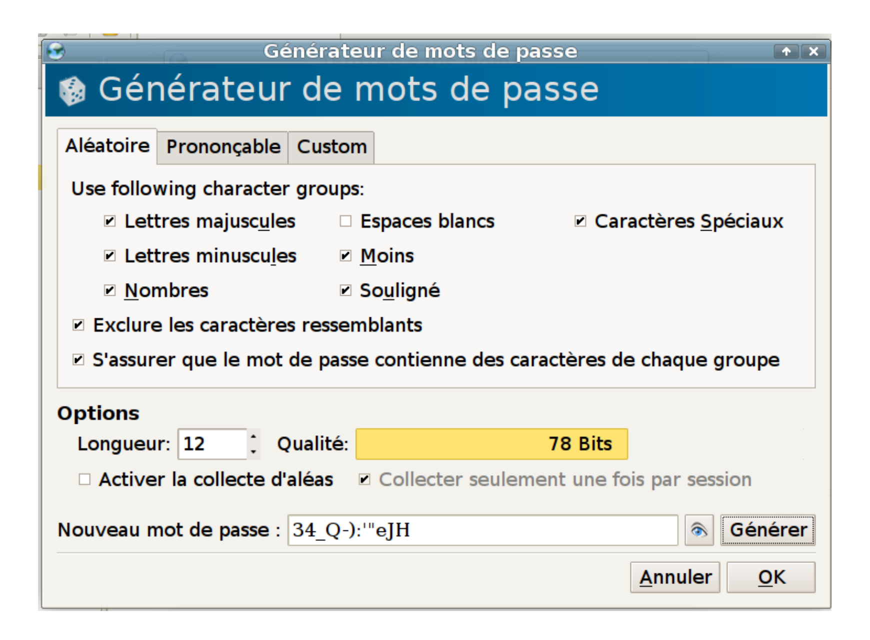
KeePassX


/home/jschaeff/.keepass.kdb (locked) - KeePassX
Fichier Entrées Groupes Affichage Extras Aide
/home/jschaeff/.keepass.kdb
Entrer la clé maitre
Dernier Fichier
Entrer un mot de passe et/ou sélectionner un fichier clé.
Clé maitre
Mot de passe :
Fichier clé :
Parcourir...
Annuler
OK

KeePassX



/home/jschaeff/.keepass.kdb - KeePassX
Fichier Entrées Groupes Affichage Extras Aide
Groupes
Clés
FTP
Hosts
Internet
eMail
logins
Backup
Autres
Titre
Nom d'utili
URL
Mot de passe
Commentaires
Adagio Teas
ADSL Free Villeurbanne
Amazon.fr
AXA Banque
CERN Auth
DeLL
DELL Groupement Rec...
ELOG IUEM
FlyingBlue
IUEM cacti admin
IUEM Nagios Admin
Redmine admin
Sirhus
SIRHUS
status.net
https://subscribes...
http://www.amaz...
www.axabanque.fr
https://login.cern...
http://www1.eur...
https://dell.quadr...
http://inventech:...
http://www.airfr...
http://inventech/...
https://janus.dsi.c...
http://status.net
Copier l'utilisateur dans le presse-papier Ctrl+B
Copier le mot de passe vers le presse-papier Ctrl+C
Ouvrir l'URL Ctrl+U
Copier l'URL vers le presse-papiers Ctrl+I
Enregistrer la pièce jointe sous...
Exécuter la Saisie Automatique Ctrl+V
Ajouter une nouvelle entrée... Ctrl+Y
Modifier/Afficher l'entrée... Ctrl+E
Dupliquer l'entrée Ctrl+A
Effacer l'entrée Ctrl+D
Redmine admin
Group: Internet
Username: ****
Password: ****
Attachment:
URL:
Comment:
Creation: 26/08/2010
Access: 26/08/2010
Modification: 26/08/2010
Expiration: Jamais


Générateur de mots de passe
Générateur de mots de passe
Aléatoire
Prononçable
Custom
Use following character groups:
Lettres majuscules
Espaces blancs
Caractères Spéciaux
Lettres minuscules
Moins
Nombres
Souligné
Exclure les caractères ressemblants
S'assurer que le mot de passe contienne des caractères de chaque groupe
Options
Longueur: 12
Qualité:
78 Bits
Activer la collecte d'aléas
Collecter seulement une fois par session
Nouveau mot de passe :
34_Q-):'"eJH
Générer
Annuler
OK

Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE





Éviter le hameçonnage

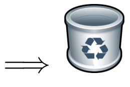
- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")





Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

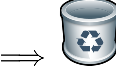
$\Longrightarrow$ 





Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

$\Longrightarrow$ 

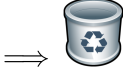
- Ne JAMAIS donner votre mot de passe à PERSONNE





Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

$\Longrightarrow$ 

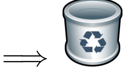
- Ne JAMAIS donner votre mot de passe à PERSONNE
- Allez directement sur le site en question plutôt que de cliquer sur un lien





Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

$\Longrightarrow$ 

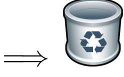
- Ne JAMAIS donner votre mot de passe à PERSONNE
- Allez directement sur le site en question plutôt que de cliquer sur un lien
- Vérifiez que l'URL corresponde bien au site





Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

$\Longrightarrow$ 

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Allez directement sur le site en question plutôt que de cliquer sur un lien
- Vérifiez que l'URL corresponde bien au site
- N'entrez vos logins/mot de passe QUE si la connexion est sécurisée

univ-brest.fr https://tucuxi.univ-brest.fr/

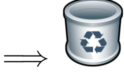






Éviter le hameçonnage

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Méfiez vous des courriels "officiels" qui ne vous nomment pas ("Cher client", "Madame monsieur")
- Si un courriel est en mauvais français

$\Longrightarrow$ 

- Ne JAMAIS donner votre mot de passe à PERSONNE
- Allez directement sur le site en question plutôt que de cliquer sur un lien
- Vérifiez que l'URL corresponde bien au site
- N'entrez vos logins/mot de passe QUE si la connexion est sécurisée





- Utilisez un navigateur récent



Changer son mot de passe sur l'ENT de l'UBO

UBO université de bretagne occidentale

Actualités Assistance Utilisateur Services Vie Etudiante Aides Mon Bureau Bibliothèques

Ma messagerie
Ancien agenda
Nouvel agenda en test
Mes réunions
Mes documents
Mes documents partagés
Logiciels en ligne
Enseignement à distance
Ressources en ligne
Mes signets
Mon dossier
Mon compte

Mon compte

Mon compte

Bienvenue sur l'espace de gestion de votre

Cette rubrique vous permet de gérer votre compte informatique à l'Université (mot de pas
D'autres fonctionalités s'ajouteront progressivement.

Vous pouvez

- changer votre mot de passe...
- rediriger votre adresse email...
- consulter vos alias de messagerie (ie. vos adresses email)...
- consulter la liste de vos listes de diffusion...
- mettre vos coordonnées sur "liste rouge"...
- consulter votre quota de messagerie...
- mes pages perso...
- comment accéder à mon espace de stockage...





Changer son mot de passe sur l'ENT de l'UBO

UBO université de bretagne occidentale

Actualités Assistance Utilisateur Services Vie Etudiante Aides Mon Bureau Bibliothèques

Mon compte

Bienvenue sur l'espace de gestion de votre

Cette rubrique vous permet de gérer votre compte informatique à l'Université (mot de pas
D'autres fonctionalités s'ajouteront progressivement.

Vous pouvez

- changer votre mot de passe...
- rediriger votre adresse email...
- consulter vos alias de messagerie (ie. vos adresses email)...
- consulter la liste de vos listes de diffusion...
- mettre vos coordonnées sur "liste rouge"...
- consulter votre quota de messagerie...
- mes pages perso...
- comment accéder à mon espace de stockage...

- Ma messagerie
- Ancien agenda
- Nouvel agenda en test
- Mes réunions
- Mes documents
- Mes documents partagés
- Logiciels en ligne
- Enseignement à distance
- Ressources en ligne
- Mes signets
- Mon dossier
- Mon compte

Mon compte





Changer son mot de passe sur l'ENT de l'UBO

Mon compte

Changement de votre mot de passe.

Saisissez votre nouveau mot de passe :

Confirmez votre nouveau mot de passe :

terminer annuler

Comment créer un bon mot de passe :

- Il a une taille d'au moins 8 caractères.
- Il contient, au moins, des minuscules ou majuscules ET des chiffres ou des caractères spéciaux (ex : %[$!/)
- Il ne contient pas votre identifiant.
- Il ne contient pas un mot concernant une donnée personnelle (votre nom, numéro de téléphone, votre code postal...)
- Il ne contient pas de mot pouvant exister dans un dictionnaire (dictionnaires français, anglais, noms communs, nom propre...)
- Il ne doit avoir une signification que pour celui qui l'a créé de façon à le retenir facilement.

Voilà, on ne va pas vous proposer de méthode pour construire ce genre de mot de passe. Votre méthode sera la meilleure pour vous, pour que vous reteniez le vôtre.

Retenez-le par coeur : votre mot de passe doit être difficile à trouver, mais facile à retenir.

Ne l'inscrivez nulle part. En particulier, ne le stockez pas dans un fichier électronique (fichier des paramètres de votre client de messagerie, fichier des préférences de votre navigateur favori), et n'activez pas l'option permettant d'enregistrer votre mot de passe.

Pourquoi créer un bon mot de passe :

Tout d'abord votre mot de passe est personnel et ne doit être divulgué à aucun tiers. Il est aussi personnel que votre numéro de carte bancaire. Pourquoi ? Parce qu'il permet de lire votre courrier électronique, d'envoyer des messages électroniques sous votre nom, de consulter votre ENT, d'y consulter vos informations personnelles, d'usurper votre identité sur le réseau informatique...

En accord avec la charte informatique de l'UBO : les règles d'usages, la charte.





Questions

Merci de votre attention



